Identifikation, Verifikation und Abwehr von Signalisierungsangriffen auf nationale Mobiltelefonnetze

Präsentation auf der
6. IT-Sicherheitskonferenz

Stralsund,
26. September 2017

GSMK Gesellschaft für
Sichere Mobile
Kommunikation mbH
Marienstraße 11
10117 Berlin

www.gsmk.de

The CryptoPhone Company

Agenda

1	**Das Problem**
2	Technischer Lösungsansatz
3	Praktische Erfahrungen

Die Annahme, daß nationale Telekommunikationsnetze einen sicheren Hafen bzgl. ausländischer Spionage darstellen, trifft schon lange nicht mehr zu

The Washington Post

washingtonpost.com • $1.25

Cellphones used as secret trackers

SYSTEMS GATHER GLOBAL LOCATION DATA

Firms market technology to foreign governments

BY CRAIG TIMBERG

Makers of surveillance systems re offering governments across e world the ability to track the ovements of almost anybody ho carries a cellphone, whether ey are blocks away or on another ontinent.

The technology works by exploiting an essential fact of all ellular networks: They must eep detailed, up-to-the-minute ecords on the locations of their ustomers to deliver calls and oth- r services to them. Surveillance ystems are secretly collecting ese records to map people's trav- ls over days, weeks or longer, ccording to company marketing ocuments and experts in surveillance technology.

The world's most powerful intelligence services, such as the National Security Agency and Britain's GCHQ, long have used cellphone data to track targets around the globe. But experts say these new systems allow less technically advanced governments to track people in any nation — including the United States — with relative ease and precision.

Users of such technology type a phone number into a computer portal, which then collects information from the location databases maintained by cellular carriers, company documents show. In this way, the surveillance system

TRACKING CONTINUED ON A5

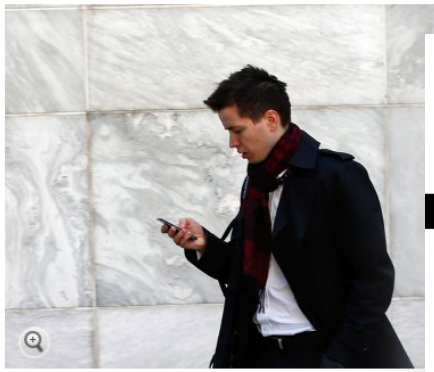
SPIEGEL ONLINE NETZWELT

Login | Registrierung

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto | Stil

Nachrichten > Netzwelt > Netzpolitik > Überwachung > SS7-Überwachung: Software ortet weltweit Mobiltelefone

Überwachung für jedermann: Firmen verkaufen Handy-Ortung weltweit



Handynutzer: Mobiltelefonortung weltweit, organisiert von Pr

Einfach zu bedienen, 70 Prozent Trefferquote: Mobiltelefonen nur auf Basis der Rufnummer, lokalisierte zum Test eine Journalistin.

Schneier on Security

Blog | Newsletter | Books | Essays | News | Schedule | Crypto | About Me

← Two New Snowden Stories | Identifying Dread Pirate Roberts →

Tracking People From their Cell Phones with an SS7 Vulnerability

What's interesting about this story is not that the cell phone system can track your location worldwide. That makes sense; the system has to know where you are. What's interesting about this story is that *anyone* can do it. Cyber-weapons arms manufacturers are selling the capability to governments worldwide, and hackers have demonstrated the capability.

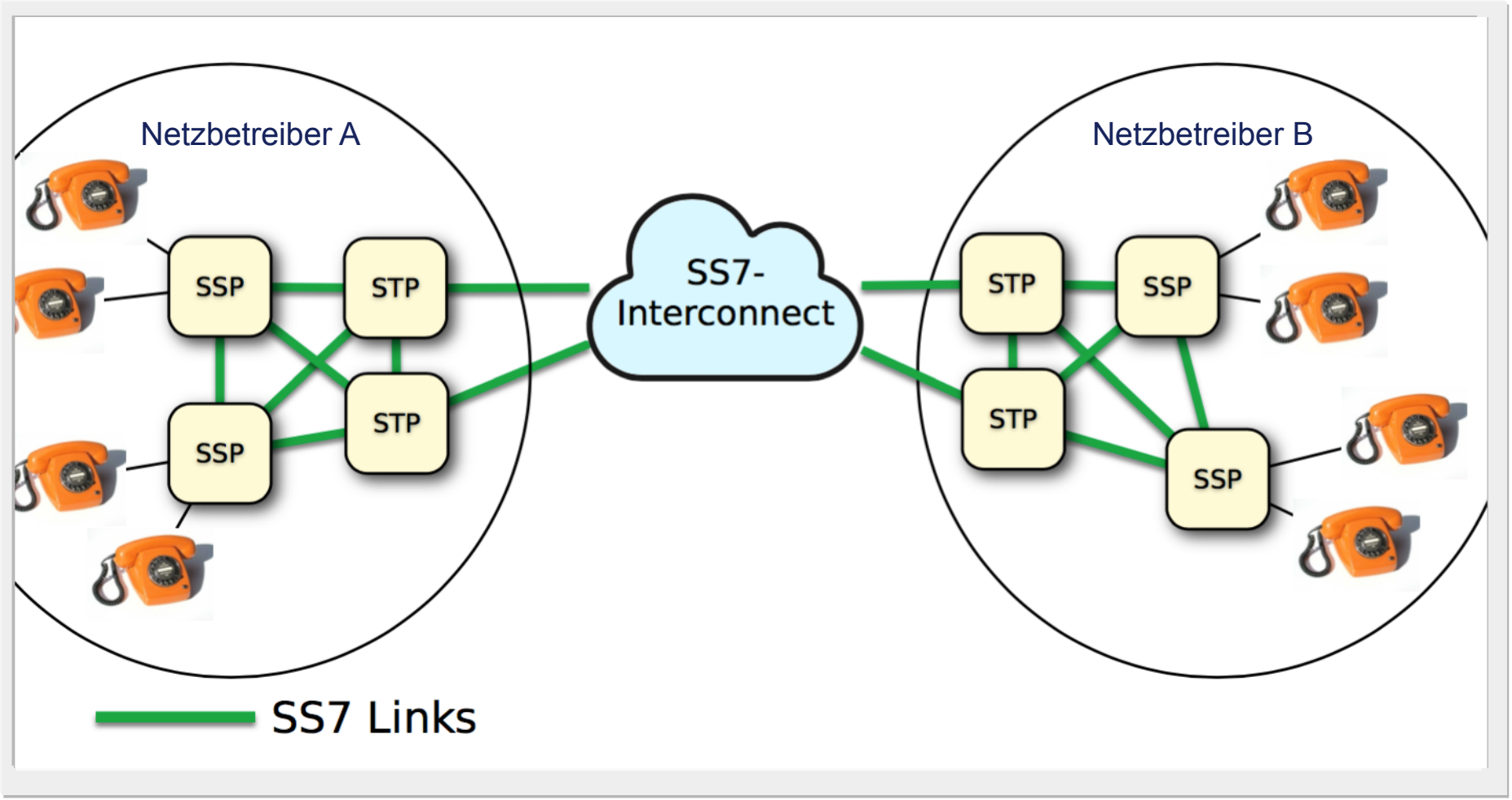
Tags: cell phones, geolocation, phones, tracking, vulnerabilities

Posted on September 17, 2014 at 7:15 AM • 22 Comments

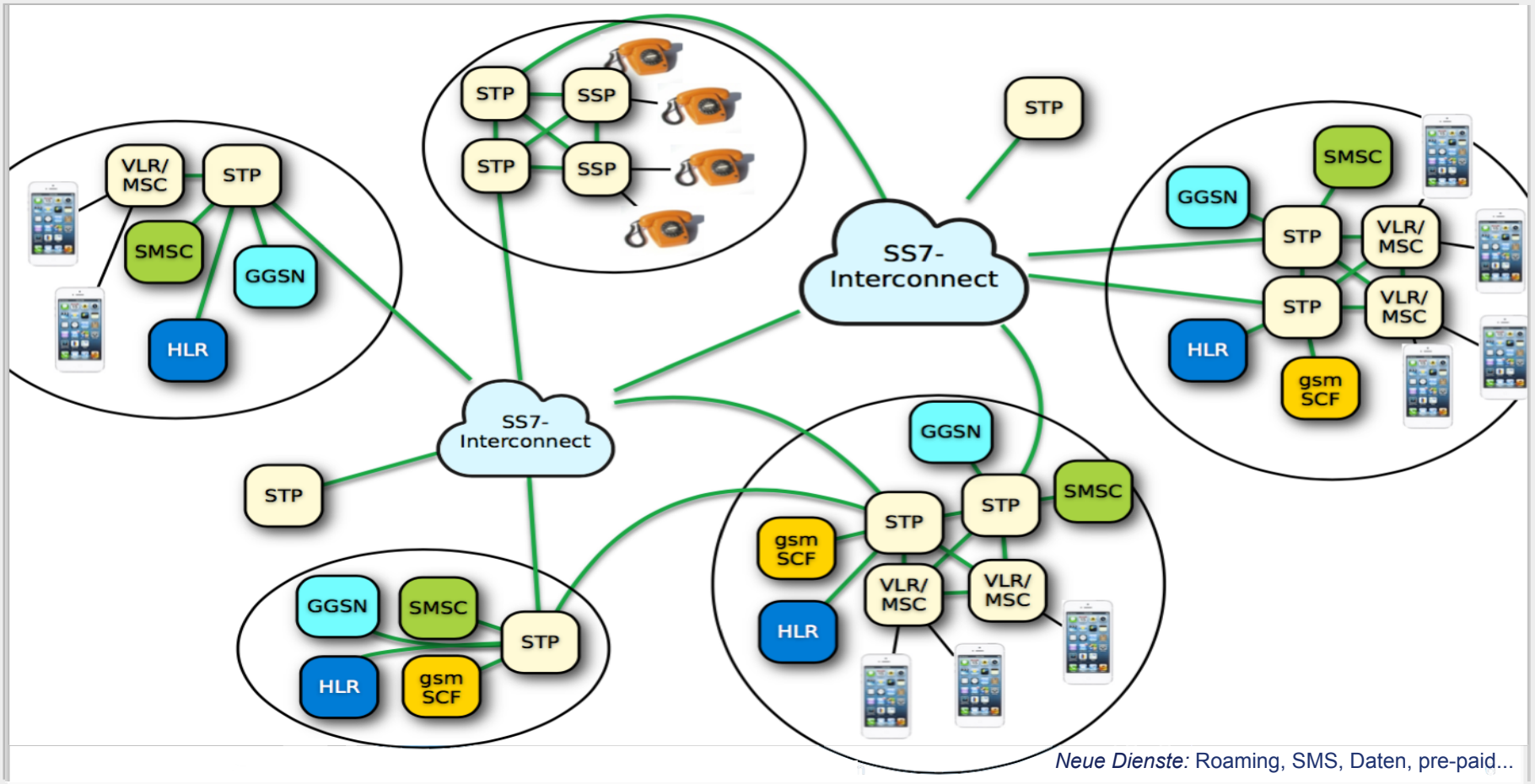
Die mehrjährigen Forschungen der GSMK haben schwere Verwundbarkeiten im Signalisierungssystem Nr. 7 („SS7“) für Sprachnetze identifiziert

- SS7-Zugangskontrollprobleme sind uns bereits seit vielen Jahren bekannt
  - Bereits im Jahre 2008 konnten wir nachweisen, daß für einen bestimmten SS7/ MAP-Befehl (sendRoutingInfoForSM) keine ausreichenden Zugangskontrollen bestehen
  - Das Anfragen einer Mobiltelefonnummer führt für jedermann nutzbar zur Übermittlung der Adresse (Global Title) der Vermittlungsstelle (MSC)
  - Da die Adresse ähnlich wie eine Mobiltelefonnummer formatiert ist, lässt sich grob der ungefähre Aufenthaltsort des Teilnehmers bestimmen
  - Mit dieser Methode sind jedoch nur die Region oder das Land des Aufenthaltsorts bestimmbar
- Seitdem haben wir zeigen können, daß SS7 auch für die straßengenaue Lokalisierung eines Mobiltelefons, Datendiebstahl und sogar das Abhören von Gesprächen aus der Ferne genutzt werden kann
- Auf Basis dieser Arbeiten kann die SS7-Kerninfrastruktur nicht mehr als vertrauenswürdig angesehen werden, was Gegenmaßnahmen erforderlich macht

Das Signalisierungsprotokoll Nr. 7 wurde ursprünglich in den 70er Jahren für nationale Fernmeldeunternehmen und Festnetzanschlüsse konzipiert...



...bevor es durch mit der Mobiltelefonie aufkommende neue Dienste und tausende von Anbietern aller Art nicht vorhergesehene Komplexität bekam



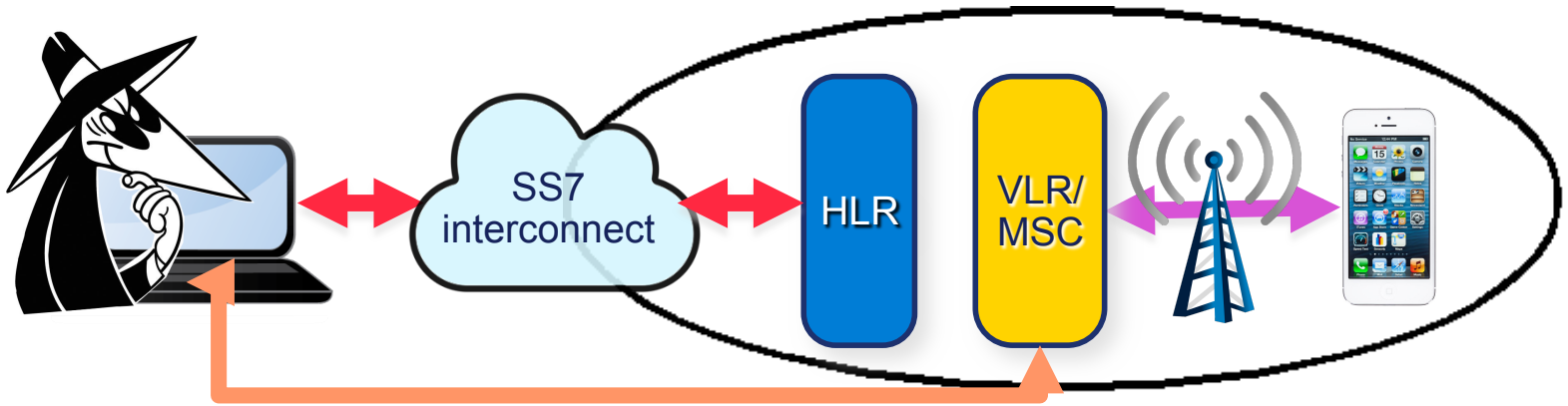
In Städten ist es dank SS7 möglich, Mobiltelefonteilnehmer bis auf Straßengenauigkeit herunter zu verfolgen

1. Angreifer fragt HLR nach aktueller VLR-Adresse für eine beliebige Rufnummer *(SS7-Kommando sendRoutingInfo)*

2. Angreifer fragt VLR nach aktueller Zelle, in der der fragliche Teilnehmer eingebucht ist *(SS7-Kommando provideSubscriberinfo)*

3. VLR initiiert Paging des Teilnehmers, um Zellen-ID zu erhalten

4. VLR gibt Zellen-ID an Angreifer zurück



- Privatsphärenverletzung erster Klasse
- Durchführbar von jedermann mit SS7-Netzzugang

Auf der Basis dieser SS7-Lokalisierungtechnik bieten bereits verschiedene kommerzielle Anbieter weltweite Ortungsdienste für Mobiltelefone an

VERINT
POWERING ACTIONABLE INTELLIGENCE®

History Module - Recalling targets past movements

The History module enables simple recollection and filtering of all SkyLock query results, alerts and notifications. This includes single queries as well as automatic (recurring queries).The main SkyLock functions which rely on the history module include:

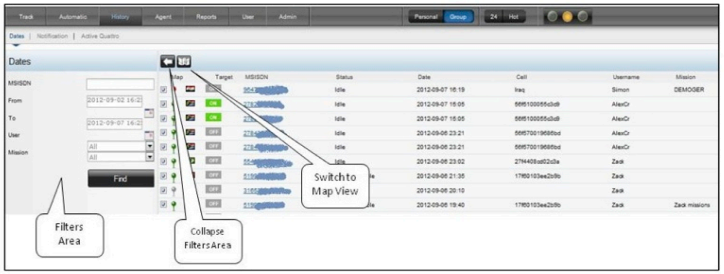


Figure 5 – SkyLock tabular History screen

Figure 6 – SkyLock map History screen

Page 10

VERINT
POWERING ACTIONABLE INTELLIGENCE®

- **Route** - Presents the route of a target, up to the last 8 queries, plotted in chronological order. This module enables tracking a target's movements over time.

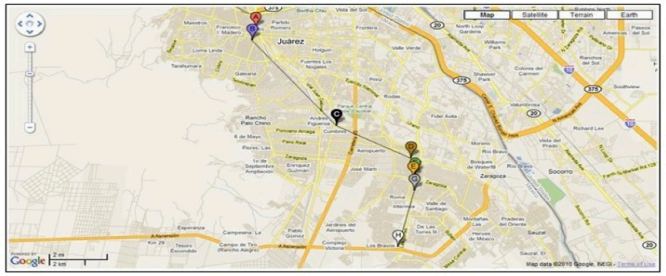


Figure 7 – Route module screen

- **Pointer** - Enables the user to detect if past target locations are nearby, and if so - This module can be used, for example, to protect a VIP figure from approaching targets, or to track a meeting between several targets in real time.

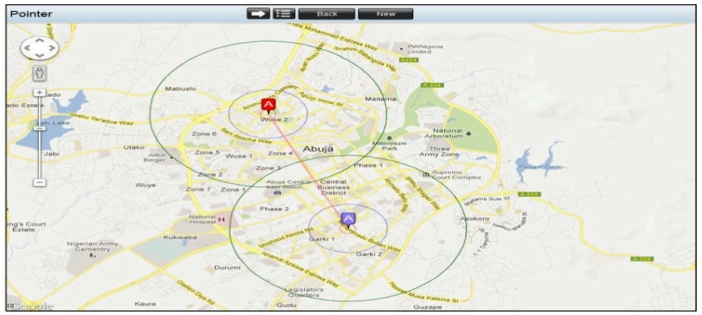
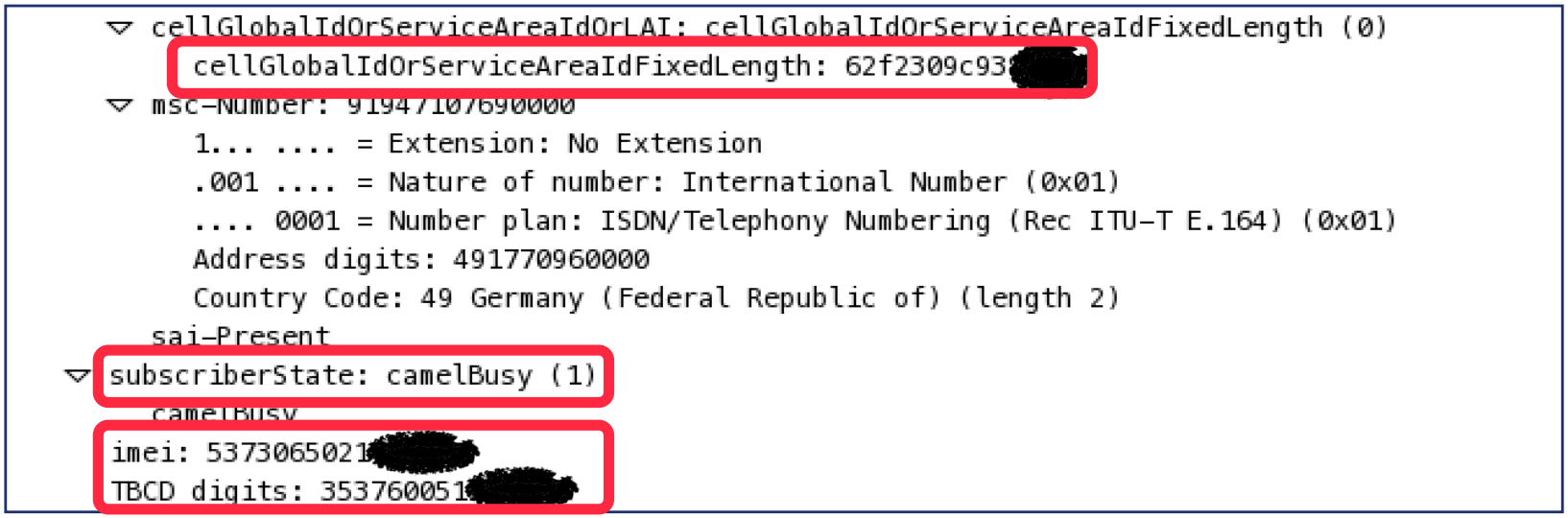


Figure 8 – Pointer module screen

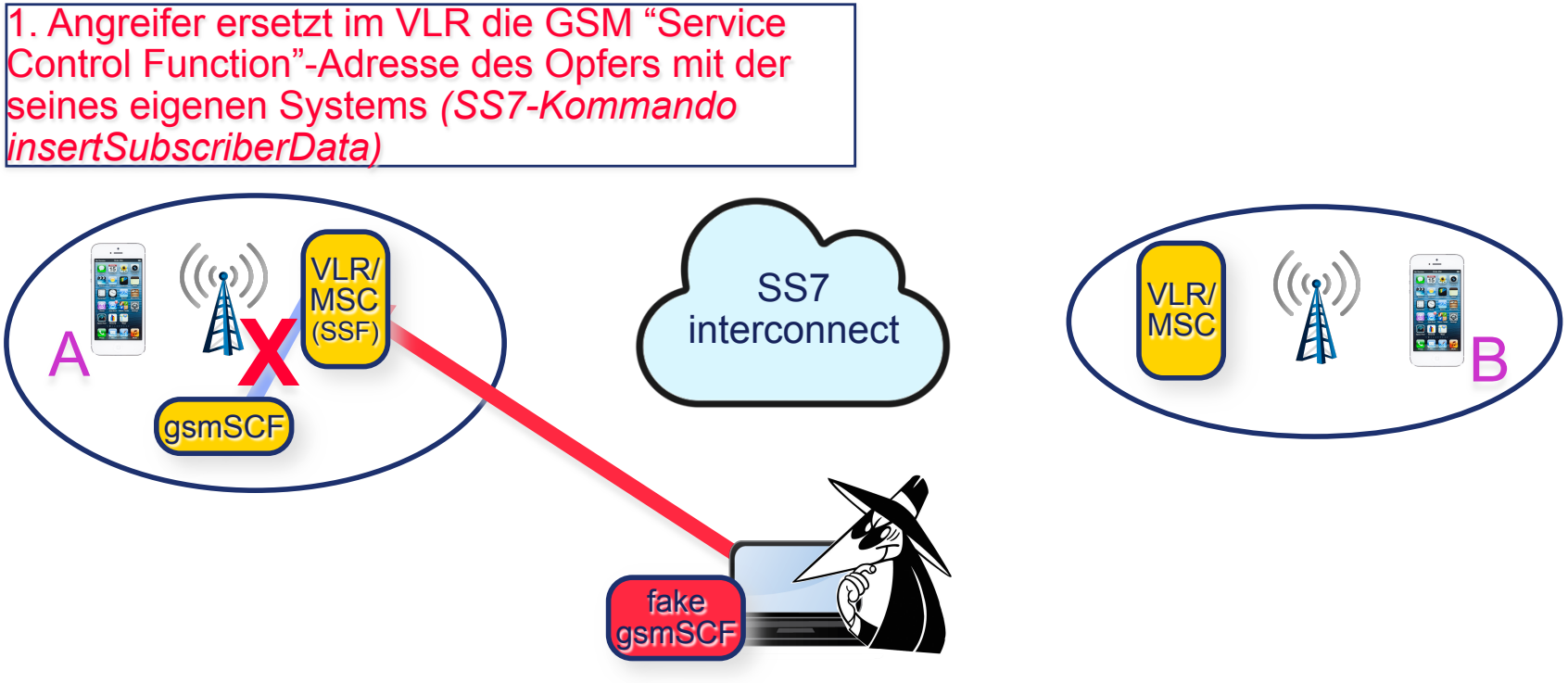
Page 11

Der gleiche Ansatz kann auch verwendet werden, um die IMEI (und damit das benutzte Telefonmodell) sowie den Teilnehmerstatus herauszufinden

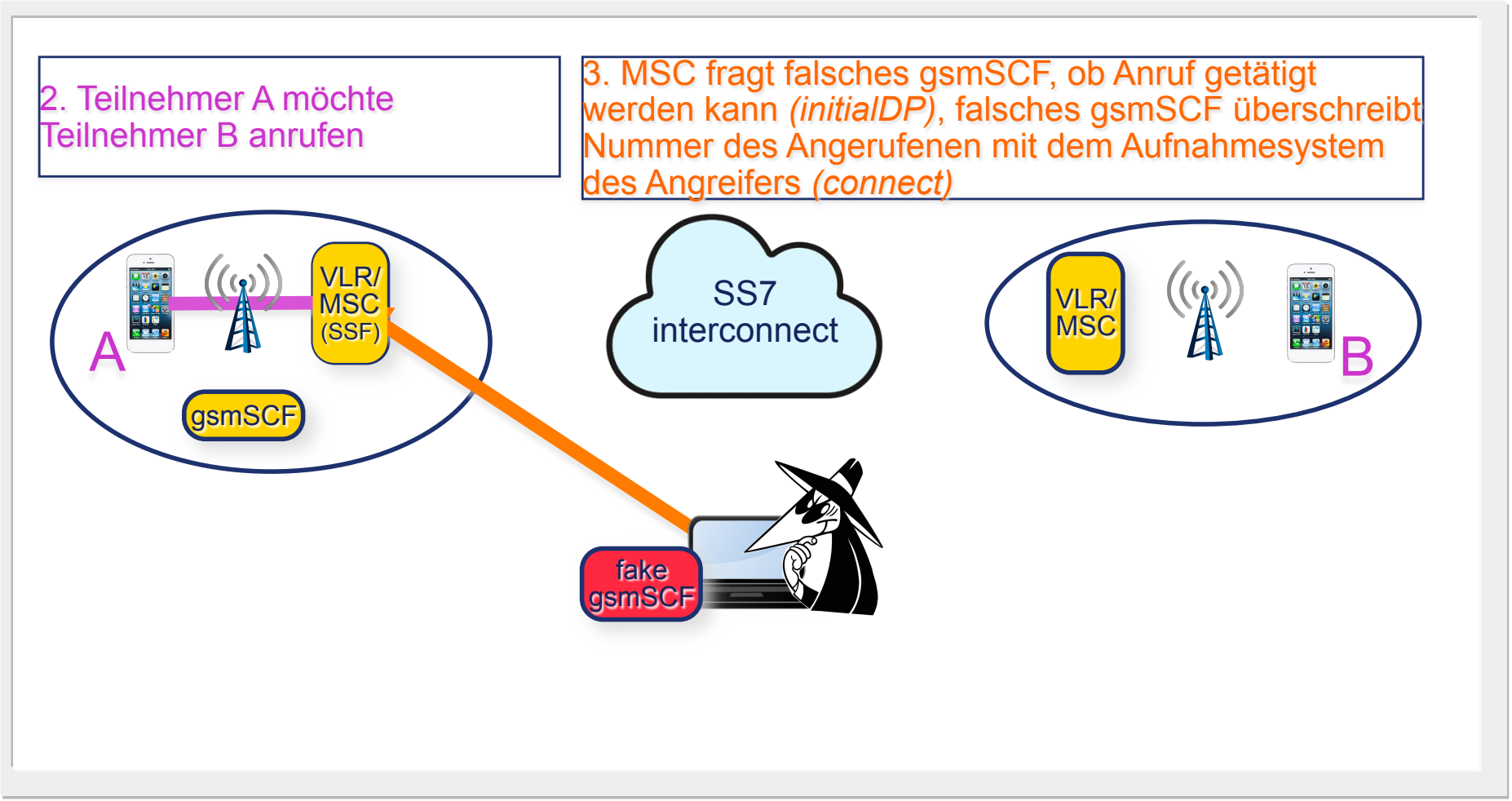
- Selbst wenn das HLR Anfragen filtert, bleibt das VLR in der Regel verwundbar
- Roaming-Vereinbarung nicht notwendig
- Teilnehmerstatus (gerade in einem Telefonat oder nicht?) ebenfalls abfragbar



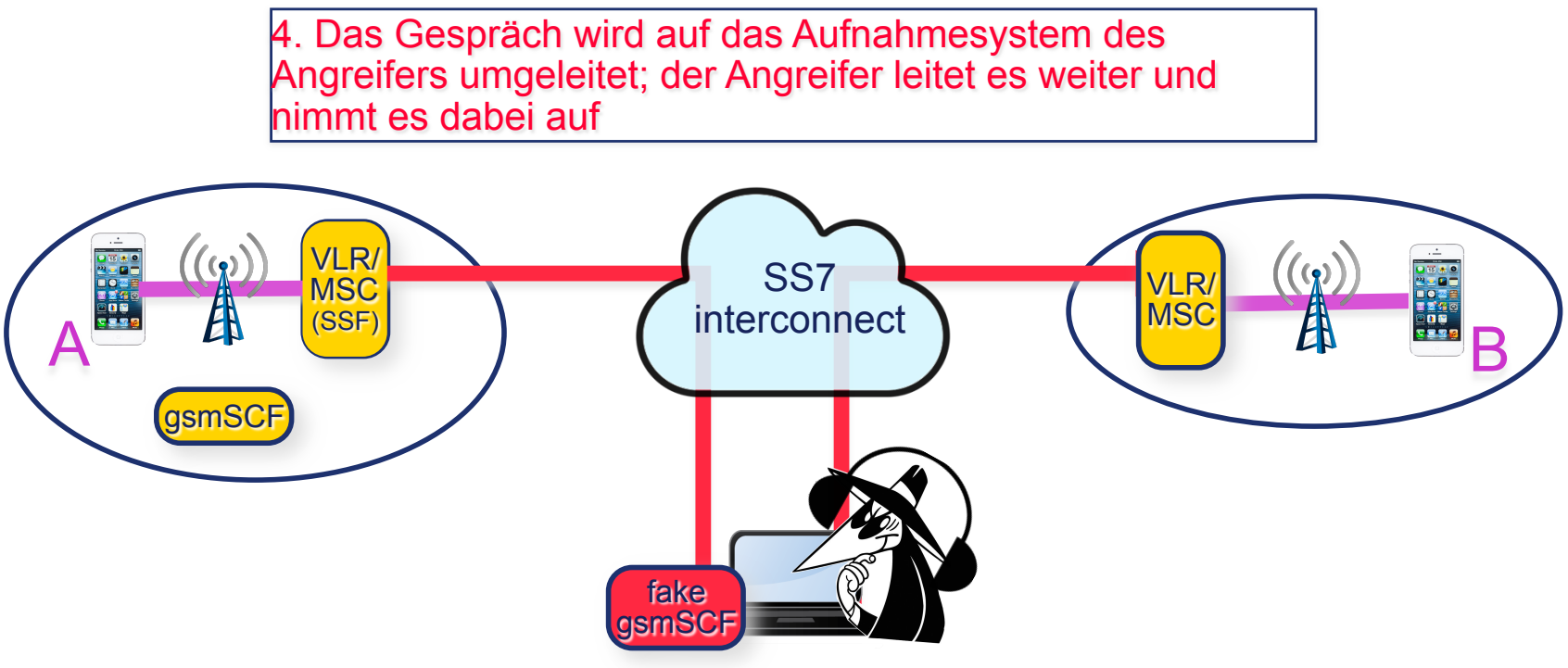
Die geschickte Ausnutzung der vorgenannten Schwachstellen erlaubt sogar das Abhören von Gesprächen aus der Ferne – ein Sicherheitsalbtraum



Die geschickte Ausnutzung der vorgenannten Schwachstellen erlaubt sogar das Abhören von Gesprächen aus der Ferne – ein Sicherheitsalbtraum



Die geschickte Ausnutzung der vorgenannten Schwachstellen erlaubt sogar das Abhören von Gesprächen aus der Ferne – ein Sicherheitsalbtraum



- Der gleiche Ansatz ist auch für SMS und Daten nutzbar!

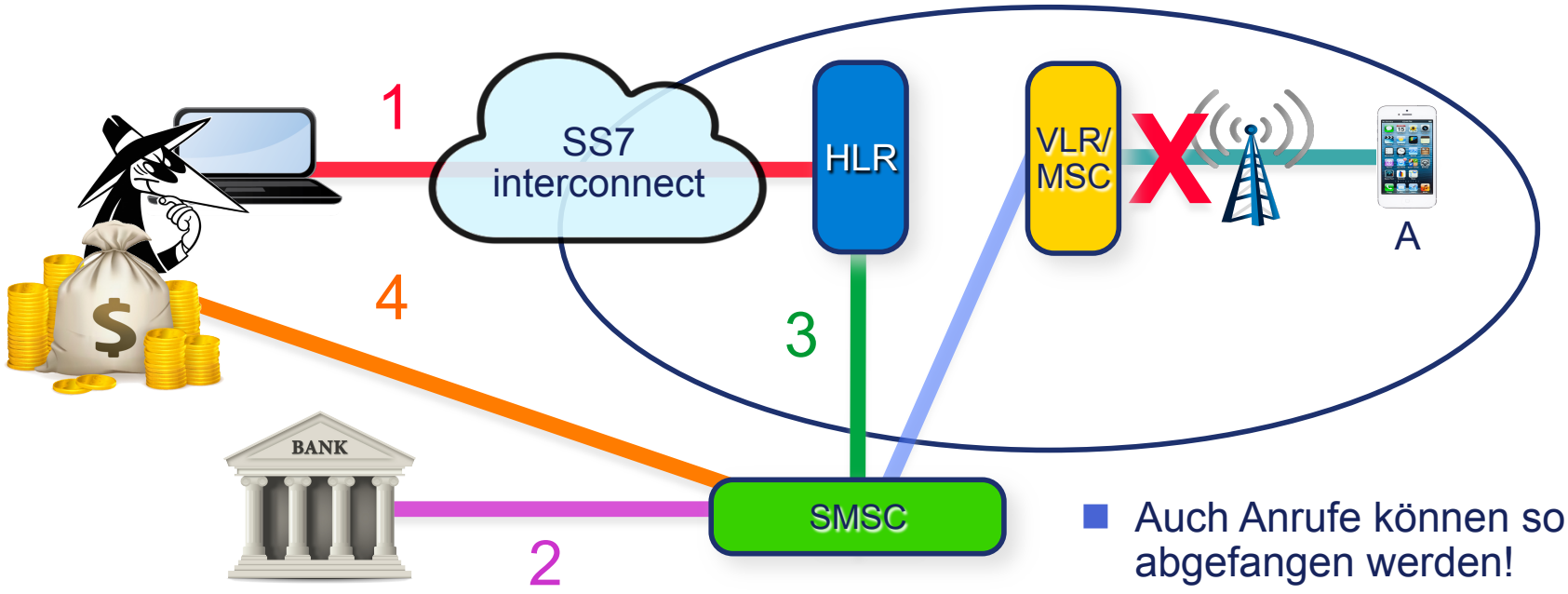
Ein verwandtes Problem ist elektronischer Bankraub duch erzwungene Umleitung von zur Authentifizierung genutzten SMS-Nachrichten (mTAN)

1. Angreifer sagt HLR, daß Teilnehmer A sich jetzt in "seinem" Netz befindet *(updateLocation)*

2. Bank sendet Textnachricht mit mTAN an Teilnehmer A

3. Das SMSC bekommt vom HLR das "VLR" des Angreifers als Ziel genannt *(sendRoutingInfoForSM)*

4. SMS wird an Angreifer ausgeliefert *(mt-ForwardSM)*



- Auch Anrufe können so abgefangen werden!

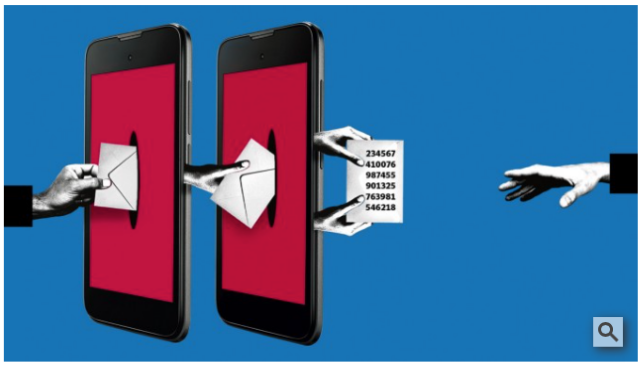
Erst als der letztgenannte Angriff vor wenigen Monaten auch in Deutschland praktisch zum Einsatz kam, fand er weitgehende Beachtung in den Medien

Süddeutsche Zeitung

Home > Digital > IT-Sicherheit > SS7: Hacker räumen Bankkonten leer

3. Mai 2017, 00:29 Uhr IT-Sicherheit

Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer



SMS von gestern Nacht. Hacker schlugen vermutlich zu, während die Opfer schliefen. *Illustration: Stefan Dimitrov.* (Foto:)

- In einem zweistufigen Angriff haben Hacker Geld von Bankkunden auf eigene Konten umgeleitet.
- Auch deutsche Kunden waren betroffen. O2-Telefonica bestätigte die Vorfälle.
- Die konkrete Schwachstelle, die von Kriminellen ausgenutzt wurde, ist seit zwei Jahren öffentlich bekannt. Die Branche hatte ausreichend Zeit, um das Problem zu lösen.

Feedback

ZEIT ONLINE

Betrüger tricksen das mTAN-Verfahren aus

Die Schwachstelle ist seit gut zwei Jahren bekannt, trotzdem konnten Kriminelle sie ausnutzen: Mit einem Trick fingen sie mTAN-SMS ab und räumten deutsche Konten leer.

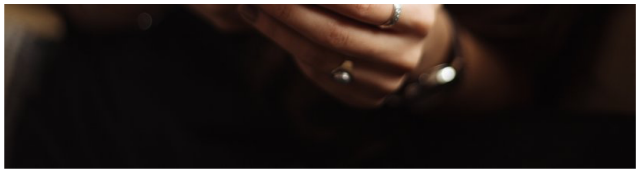
Von **Patrick Beuth**

IT Finanzmagazin

Das Fachmagazin für IT und Organisation bei Banken, Sparkassen und Versicherungen

3. Mai 2017

Das Ende der mTAN: Die Schwachstelle im Mobilfunknetz heißt SS7-Protokoll – und ist seit 2014 bekannt



Im mTAN-Verfahren bekommen Nutzer vor jeder Online-Überweisung eine SMS mit einer Transaktionsnummer von ihrer Bank, mit der sie den Zahlungsvorgang bestätigen müssen.
© I'm Priscilla/unsplash.com

SPIEGEL ONLINE

Hackerangriffe aufs mTAN-Verfahren

So schützen Sie sich beim Onlinebanking

Mit einem komplexen Angriff ist es Kriminellen offenbar gelungen, Geld von fremden Konten zu erbeuten.

Agenda

1	Das Problem
2	**Technischer Lösungsansatz**
3	Praktische Erfahrungen

Gegeben die Kenntnis dieser Möglichkeiten gilt es zum einen für Unternehmen und Verbraucher, Sofortmaßnahmen zum Eigenschutz treffen

- **Strenge Regelungen zur (Mobil-)Telefonnutzung**
  - Die unverschlüsselte Besprechung vertraulicher Inhalte am Telefon muß konsequent unterbleiben!
  - Alternativen: Sprachverschlüsselung für Mobil- und Festnetztelefone (preiswert auf App-Basis z.B. Mobile Encryption App von der Deutschen Telekom), verschlüsselte E-Mail, etc.
- **Kündigung/Änderung aller Verträge mit SMS-basierter Authentifizierung**
  - Die mTAN ist kein sicherer Authentifizierungsmechanismus für electronic banking!
  - Alle Prozesse, die SMS-Nachrichten oder Sprachanrufe als Authentifizierung verwenden, müssen auf den Prüfstand
- **Absicherung vor Betrugsversuchen**
  - In Zusammenarbeit mit Risikomanagement / Rechtsabteilung TK-Verträge überprüfen: Wer haftet bei SS7-basiertem Betrug?

Die eigentliche Lösung des Problems muß beim Netzbetreiber stattfinden, was umfangreiche Auswertung und Filterung des SS7-Verkehrs erfordert

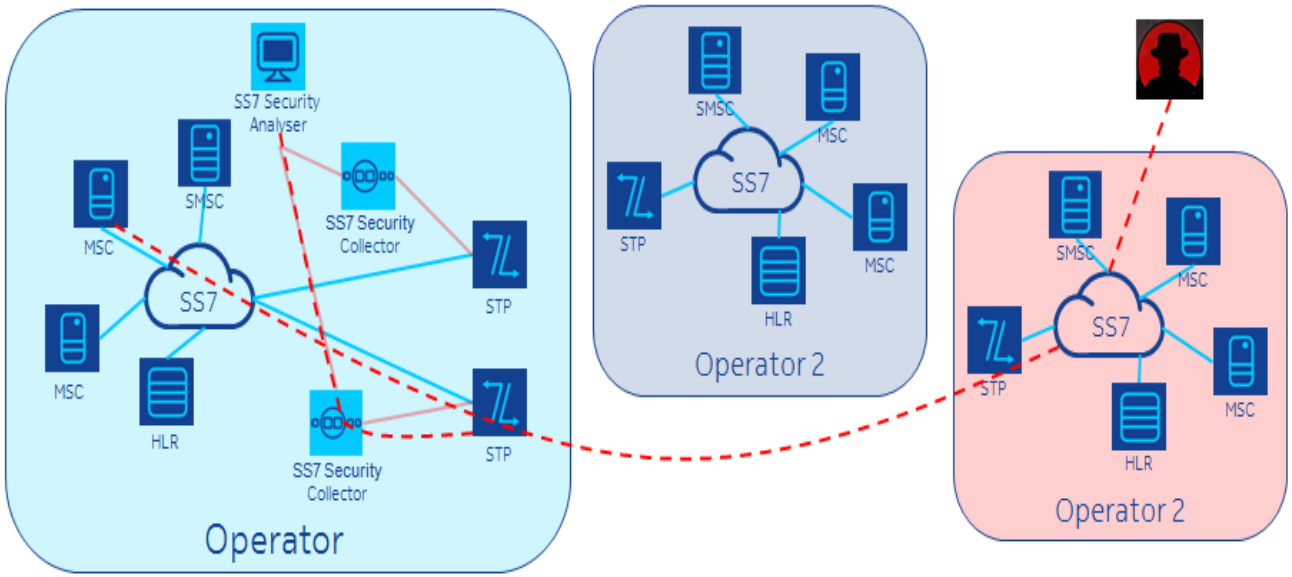
- Allgemeine Vorsichtsmaßnahmen, z.B.:
  - Viele Operationen wie *anyTimeInterrogation* oder *sendIdentification* sind nur für den internen Einsatz spezifiziert ➔ Alle netzinternen Anfragen an den Interconnection Points filtern
  - Der Angreifer benötigt meist die IMSI sowie die Adresse des derzeitigen VLR/MSC/ SGSN des Teilnehmers ➔*SMS Home Routing einführen, um solche Informationen zumindest nicht mehr wahllos preiszugeben*
- Mittel- und langfristig notwendige Maßnahmen zur Angriffserkennung und -abwehr:
  - Eine dauerhaft wirksame Abwehr muß über simple Filtermaßnahmen hinausgehen und in der Lage sein, über verschiedene Protokollschichten (SS7, MAP, CAP) hinaus Aussagen über die Legitimität des beobachteten SS7-Netzverkehrs treffen können
  - Für dieses Ziel entwickelte SS7 Angriffserkennungs- und Abwehrsysteme dürften in wenigen Jahren analog zur im IP-Umfeld lange geübten Praxis Standard werden
  - In den folgenden Folien wird anhand eines solchen neuentwickelten Systems exemplarisch gezeigt, wie das Problem technisch gelöst werden kann

Neuer Lösungsansatz: SIGTRAN-basiertes System zur Angriffserkennung und -abwehr durch Analyse von Verkehrsranddaten

- **Verteilte Erfassung und Aufbereitung der Daten** durch sog. „Detector Nodes“, die an die SS7 Signal Transfer Points (STPs) angeschlossen werden
- **Zentrale Auswertung und Visualisierung** macht gewonnene Verkehrsranddaten nutz- und analysierbar
  - **Aggregation der Daten** aller angeschlossenen STPs, womit auch Angriffe erkannt werden, die zur Angriffsverschleierung unterschiedliche STPs nutzen
  - **Analyse aller relevanten Nutzlasten**, STP-übergreifende Extraktion von SCCP-Adressierung, TCAP-Transaktionskennungen und Dialogkomponenten
  - Analyse und **Korrelation über Protokollschichten hinweg**
  - Anwendung eines Regelsystems auf die aus den Signalisierungsdaten extrahierten Metadaten zwecks **Klassifikation der jeweiligen Nachricht**
  - Klassifikation löst **Aktionen für Protokollierung, Alarmierung und Visualisierung** der identifizierten Angriffe aus

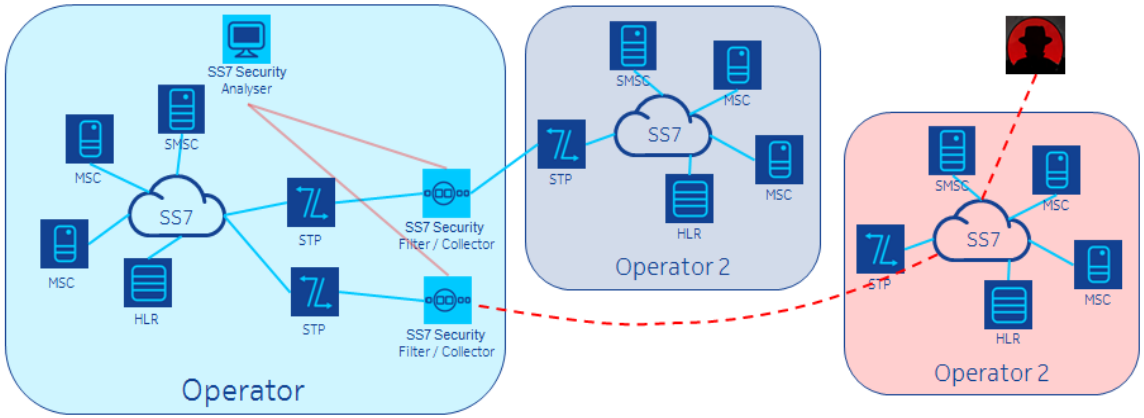
Der Weg über passive Beobachtung der Verkehrsranddaten ermöglicht ein Intrusion Detection System ohne grundlegende Änderungen am Netz

- Einfache Kopie der Daten wird den Collector Nodes zur Verfügung gestellt, z.B. durch Portspiegelung, Datenabfluß oder kleine Konfigurationsänderung am STP
- Analyse und Visualisierung wie vorab erläutert an zentraler Stelle (“Oversight Manager”), so daß Informationen von mehreren STPs integriert werden können
- (Geo-)Redundanz sowohl auf der Collector- als auch der Analyse-ebene unterstützt

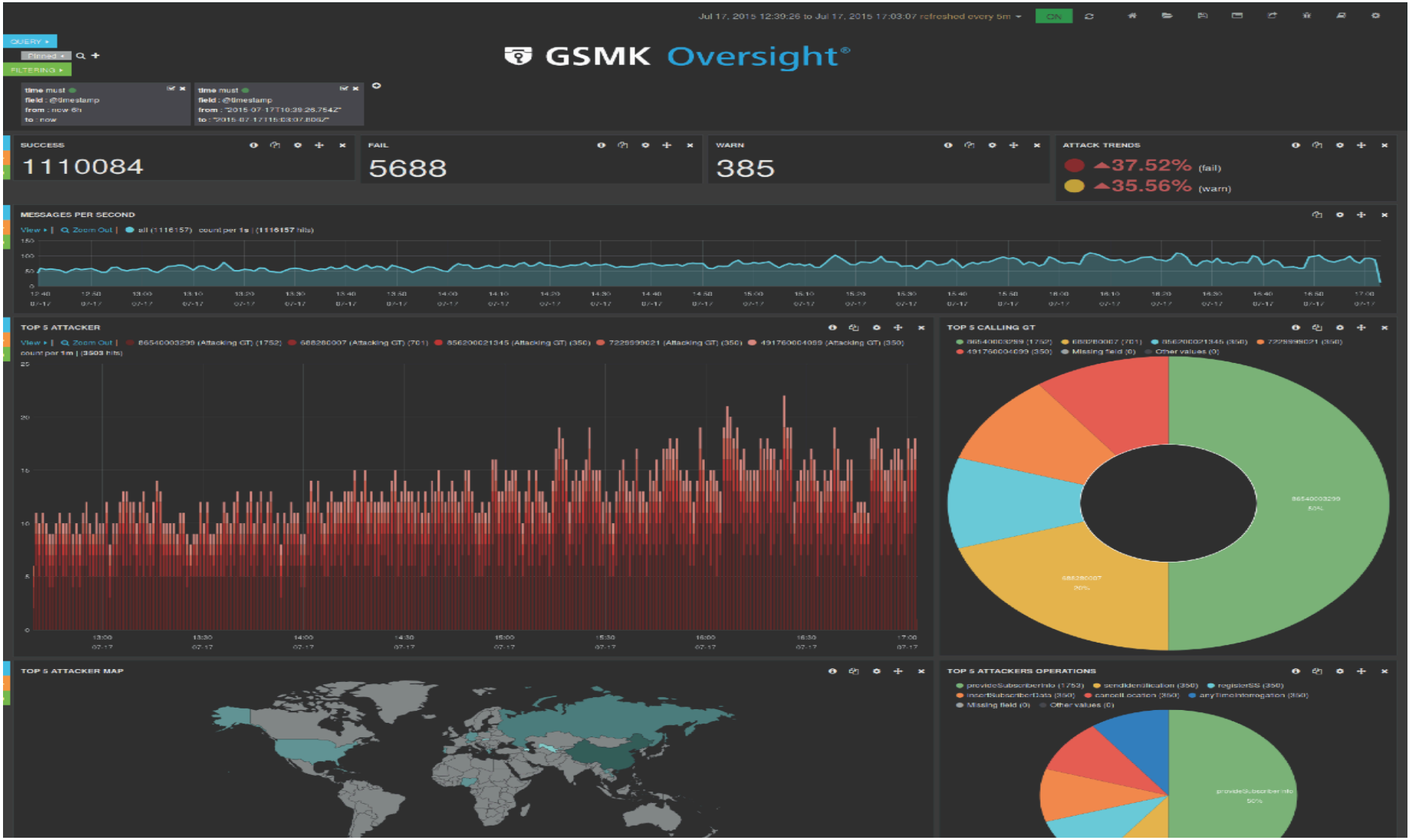


Wenn die Detector Nodes aktiv in den Signalpfad eingeschliffen werden, ist auch eine automatisierte Abwehr von Angriffen i.S. einer Firewall möglich

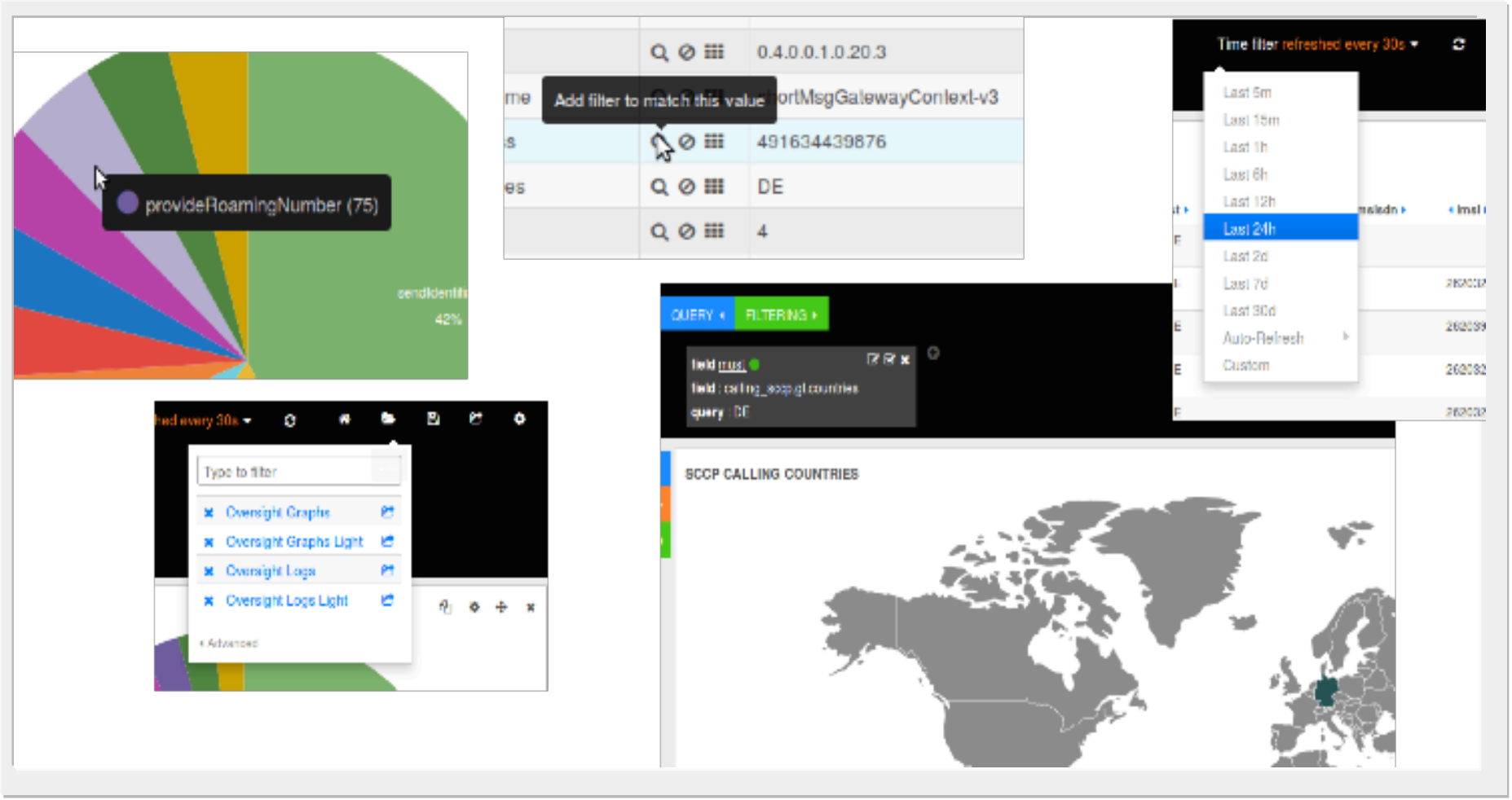
- Intrusion *Protection* System erfordert aktive Eingriffe in den Signalpfad, um als Teil eines Angriffs identifizierte Nachrichten blockieren oder fallenlassen zu können
- Basierend auf der gleichen Analysekomponente wie das IDS kann ein IPS entsprechende Aktionen ausführen, inkl. Filterung mittels Whitelist/Blacklist
- Hier vorgestelltes System erlaubt über flexible Filterkonfigurationssyntax Aktionen wie Löschen, Erfassung, Alarmierung usw.



Ein leistungsstarkes Visualisierungssystem erlaubt dann Filterkonfiguration, Filtergruppierung, Graphen, Logs, Berichte und Systemadministration



Es hat sich als sinnvoll erwiesen, das GUI voll konfigurierbar & adaptierbar zu halten, um netzbetreiberspezifische Anforderungen abdecken zu können



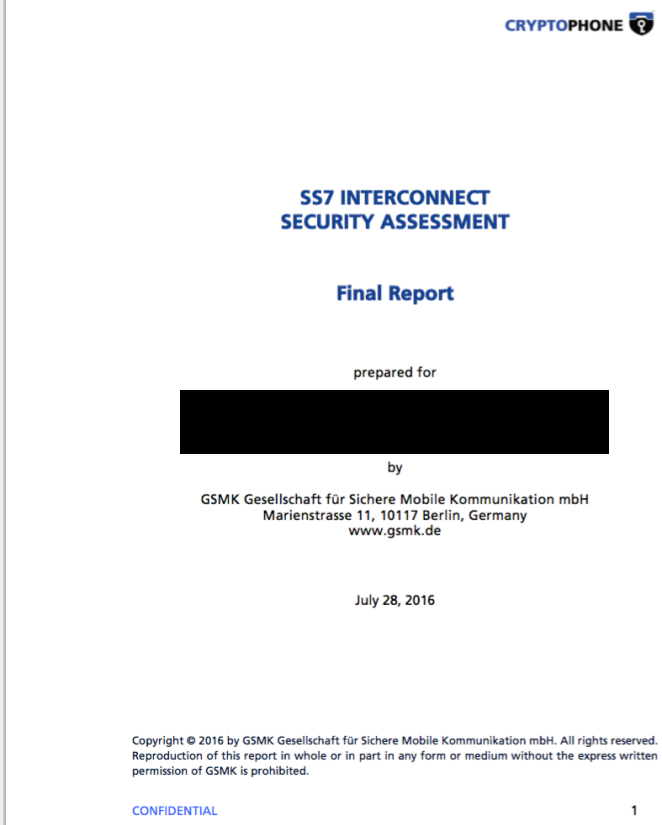
Agenda

1 Das Problem

2 Technischer Lösungsansatz

3 Praktische Erfahrungen

Die Untersuchung realer Verwundbarkeiten hat bei jedem analysierten Netzbetreiber jeweils schwerwiegende Verwundbarkeiten offenbart



CRYPTOPHONE

SS7 INTERCONNECT
SECURITY ASSESSMENT

Final Report

prepared for

[redacted]

by

GSMK Gesellschaft für Sichere Mobile Kommunikation mbH
Marienstrasse 11, 10117 Berlin, Germany
www.gsmk.de

July 28, 2016

CONFIDENTIAL 1

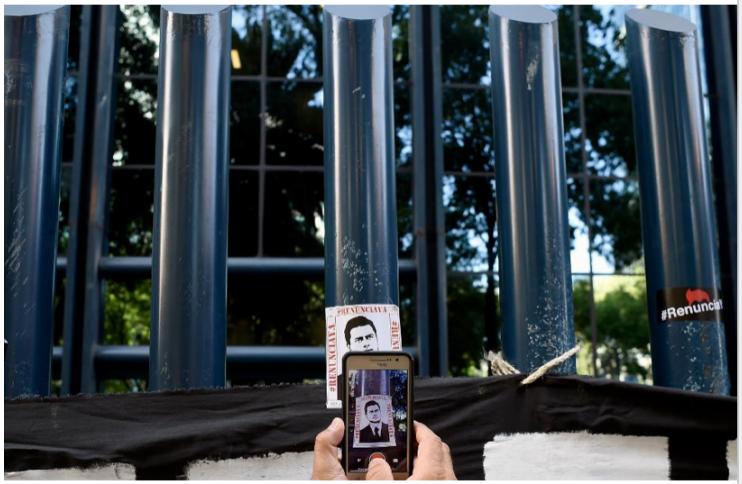
- **Datenbasis:** SS7-Penetrationstests und Verwundbarkeitsanalysen für **Netzbetreiber in Europa, Nordamerika und Asien**
  - Seit 2015 große Anzahl von Studien im Auftrag der jeweiligen Netzbetreiber
  - Kunden umfassen u.a. **alle Tier 1-Netzbetreiber in den USA** und **fast alle Tier 1-Netzbetreiber in Europa**
- GSMK repliziert SS7-Verwundbarkeiten, um dem Netzbetreiber besseres Verständnis von **Risiko und Gefährdungsgrad der eigenen SS7-Topologie** zu ermöglichen
- **Jede** einzelne Untersuchung hat dabei **bei jedem analysierten Netzbetreiber** jeweils schwerwiegende Verwundbarkeiten im Bereich der Signalisierungstechnik offenbart

Jeder der das Angriffserkennungssystem einsetzenden Netzbetreiber war von Quantität und Qualität der Angriffe und Betrugsfälle überrascht

- ***Größe des Problems erst durch Angriffserkennungssystem erkannt***
  - Angriffe in signifikantem Anteil des Gesamtverkehrs, vorher unentdeckt
  - Zwei Hauptarten von Angriffen: Staatliche Akteure (Informationen) und kriminelle Organisationen (v.a. Betrug)
  - Beifang: Nicht vertragskonformes Verhalten von Roaming-Partnern
- ***U.S. Senat hat Untersuchung eingeleitet***
  - Tiefgreifende Bedenken bzgl. des Umgangs mit flächendeckenden Verwundbarkeiten einer kritischen Telekommunikationsinfrastruktur
  - Staatliche Vorgaben wahrscheinlich

Forbes-Meldung vom 25.09.2017

Did Mexico Drop $5 Million On This 'Unlimited' Uber-Stealth Spy Tech?



Mexicans protest at mobile surveillance of journalists and activists in the country in June 2017. President Enrique Peña Nieto has called for an inquiry into use of an Israeli spy tool called Pegasus, but now it appears a new, even more powerful surveillance tool has been purchased by the country. (Credit: ALFREDO ESTRELLA/AFP/Getty Images)

Mexico is one of the biggest buyers of next-generation surveillance technology. And now data leaked to *Forbes* indicates it's taken an unprecedented step in becoming the first known buyer of surveillance technology that silently spies on calls, text messages and locations of any mobile phone user, via a long-vulnerable portion of global telecoms networks known as Signalling System No. 7 (SS7).

Die Schwere der SS7-Probleme erfordert, daß sowohl Unternehmen als auch Netzbetreiber ihre Einstellung zur Netzsicherheit nachhaltig überdenken

- ***Hohe Signifikanz des Problems***
  - Die SS7-Kerninfrastruktur kann nicht länger als vertrauenswürdig angesehen werden – mit weitreichenden Konsequenzen für Privatsphäre und Sicherheit
  - Gleichzeitig lässt sich aber vermutlich auf Jahrzehnte hinaus nicht auf diese Infrastruktur verzichten
- ***Sofortmaßnahmen für Unternehmen und Verbraucher***
  - Strenge Regelungen zur (Mobil-)Telefonnutzung, Verschlüsselung einsetzen
  - Kündigung/Änderung aller Verträge mit SMS-basierter Authentifizierung
- ***Lösungsansätze auf Netzbetreiberseite***
  - Verkehrskreise einschränken, Filtern des SS7-Verkehrs
  - Einführung von Angriffserkennungssystemen und SS7 Firewalls

Vielen Dank für Ihre Aufmerksamkeit

Dr. Björn Rupp
Geschäftsführer
br@gsmk.de

GSMK Gesellschaft für Sichere Mobile Kommunikation mbH
Marienstraße 11
10117 Berlin
Tel +49 700 CRYPTTEL [27978835]
Fax +49 700 CRYPTFAX [27978329]
www.gsmk.de